

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-161165

(43)Date of publication of application : 18.06.1999

(51)Int.Cl.

G09C 1/00

G06F 13/00

H04L 9/32

(21)Application number : 09-325768

(71)Applicant : HITACHI LTD

(22)Date of filing : 27.11.1997

(72)Inventor : FURUKAWA ISAO

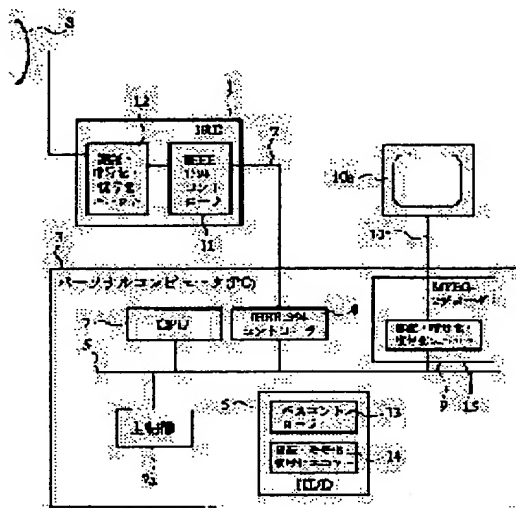
(54) INFORMATION PROCESSING DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent an unauthorized access to the data which are handled by the information processing device.

SOLUTION: The device composed of a PC3 and an antenna 8 which receives pay satellite broadcasting signals, etc., and an IRD (a digital satellite broadcasting tuner) 1, both of which are connected to the PC3 through an IEEE 1394 bus 2. IN the PC3, an IEEE 1394 controller 4 which conducts an I/F control of the IEEE 1394 bus 2, a storage device (HDD) 6 which stores the data, etc., received by the IRD 1, a CPU 7 which controls the entire system, a main storage 7a and a MPEG-2 decoder 9 for contents reproducing, etc., are connected through a PCI bus 5. In such a constitution, each of the HDD6, the IRD1 and the decoder 9 is provided with a certifying.ciphering.deciphering unit 14, that certifies the party to which data are transmitted, and certifying.ciphering.deciphering units 12 and 15.

Then, certifying of each among the units 12, 14 and 15 and data ciphering/deciphering of the data, which are flowing in the data transfer paths including the buses 2 and 5, are conducted.



LEGAL STATUS

[Date of request for examination] 31.08.2000

[Date of sending the examiner's decision of rejection] 06.04.2004

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

特開平11-161165

(43)公開日 平成11年(1999)6月18日

(51)Int.Cl. ⁶	識別記号	F I
G 0 9 C 1/00	6 2 0	G 0 9 C 1/00 6 2 0 Z
G 0 6 F 13/00	3 5 7	G 0 6 F 13/00 3 5 7 A
H 0 4 L 9/32		H 0 4 L 9/00 6 7 5 B

審査請求 未請求 請求項の数1 O L (全 8 頁)

(21)出願番号 特願平9-325768

(22)出願日 平成9年(1997)11月27日

(71)出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72)発明者 古川 勲

神奈川県海老名市下今泉810番地 株式会

社日立製作所オフィスシステム事業部内

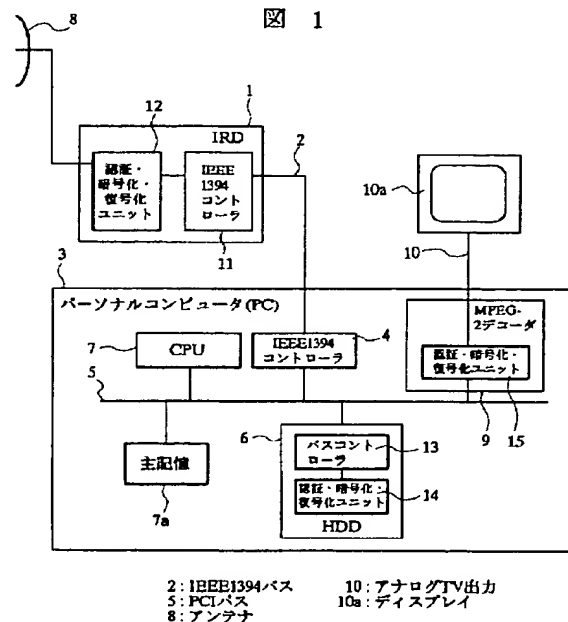
(74)代理人 弁理士 筒井 大和

(54)【発明の名称】 情報処理装置

(57)【要約】

【課題】 情報処理機器にて取り扱われるデータの不正使用を防止する。

【解決手段】 PCIバス5を介して、IEEE1394バス2とのI/F制御等を行うIEEE1394コントローラ4、IRD1にて受信されたデータ等の格納を行う記憶装置(HDD)6、全体の制御を行うCPU7、主記憶7a、コンテンツ再生用のMPEG-2デコーダ9等を接続した構成のPC3に、有料衛星放送等の受信を行うアンテナ8、IRD1をIEEE1394バス2を介して接続した構成において、HDD6、IRD1、MPEG-2デコーダ9の各々には、データの送信相手の認証等の動作を行う認証・暗号化・復号化ユニット14、認証・暗号化・復号化ユニット12、認証・暗号化・復号化ユニット15を設け、これら3者間における互いに他の認証、IEEE1394バス2やPCIバス5等のデータ転送路を流れるデータの暗号化/復号化を行うようにした。



【特許請求の範囲】

【請求項 1】 所望の情報伝送路を介して記憶装置と周辺機器とが接続された構成の情報処理装置であって、前記記憶装置および前記周辺機器の各々には、前記情報伝送路を経由して情報の授受を行う相手側を認証する第 1 の機能、および前記情報伝送路を経由して授受される前記情報の暗号化および復号化を行う第 2 の機能の少なくとも一方を備えたことを特徴とする情報処理装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、情報処理技術に関し、特に、たとえばパーソナルコンピュータ等の情報処理機器にて取り扱われるデジタルコンテンツ等のデータの保護に適用して有効な技術に関する。

【0002】

【従来の技術】映画や音楽などの多量のデータを不正コピーから守る技術として、コピープロテクトのための技術が多数開発されている。代表的なものはビデオテープにおけるアナログコピープロテクトで、NTSC規格の映像信号に規格外の信号を与え、ビデオの誤動作を引き起こすものである。代表的なものとしてMacroVision社のプロテクトがある。また、DAT(Digital Audio Tape)の場合は、世代管理のための記憶領域が設けられており、コピー不能、1回のみコピー可能、何回でもコピー可能といったようにコピー世代を指定できる。これは、データ自体への暗号化は為されておらず、DATの機械には必ずコピー管理機構を設けることを義務づけること、および媒体であるテープへ一定の課金をするという手法をとっている。また、デジタル衛星放送の一つであるPerfectV!においては、PerfectCardと呼ばれるICカードをIRD(デジタル衛星放送チューナ)に差し込まないと有料放送が見れない、というガードがある。ICカードには固有のIDがあり、特定のチャンネルには特定のPerfectCardのIDしか見れないように放送局側で規制している。IRDはPerfectCardのIDと番組情報から、これをデコードして良いか判断するものである。

【0003】一方、コンピュータの世界では、また別のコピープロテクト技術がある。代表的なものとしては、

【0004】CD-ROMやFDの分野では、物理フォーマットの特性を利用したプロテクトが行われている。これは、規格外のFDやCD-ROMを作り、コントローラ等のハードウェアをプログラム自らが制御して、本来読めないはずの規格外のエリアにあるデータがあるかどうかで正規のメディアかどうかを確認するものである。

【0005】また、比較的高価なCADソフトの一部では、PC(パーソナルコンピュータ)の平行ポート

に接続する専用キーデバイスによるプロテクトがある。これは、CADソフトの販売元から正規のユーザに配付され、平行ポートに接続するコネクタの形状を呈する認証装置であり、やはり固有のIDを持っている。CADソフトは平行ポートに装着されたこの認証装置のIDを読み取り、正規のID(ユーザ)であるかどうかを判断して動作するかどうかを決めるというものである。

【0006】ソフトのインストールや起動の際にパスワードを入力するという手法も広く行われている。

【0007】DVDやデジタル衛星放送の出現により、映像や音声、データなどのコンテンツがデジタルで配信される機会が急速に広まっている。次世代IRDでは、このためのIRDからのデジタルデータの出力の規格としてIEEE1394を使用することがほぼ確定している。IEEE1394は次世代の高速シリアルバスの一つであり、400Mbps以上の伝送速度とPlug & Play、Hot Plugの機能を実現したバスである。また、放送の種類として、従来の音声、映像のみではなく、PC(パーソナルコンピュータ)等の個人用の情報処理機器での使用を前提としたデータ放送の予定もある。また、デジタルVTR、デジタルオーディオアンプ、等のAV機器にもIEEE1394が搭載される見込みである。

【0008】デジタルでのコピーは、いくらコピーしてもデータの劣化がないため、最初にコピーを許してしまうと後は高品質のデータのコピーし放題になるという重大な問題がある。よって、従来以上にコピープロテクトには気を使わなければならない。従来の技術では、IRDからのデータ放送は、コピープロテクトという観点ではさまざまな問題を抱えている。以下にその内容を示す。

【0009】

【発明が解決しようとする課題】ユーザが暗証番号を入れる方法では暗証番号と一緒にコピーされたりアタックされる可能性がある。これは、ユーザが入れられる暗証番号の桁数は一般的に短いことに起因するものである。また、平行ポートに接続する、あるいはPerfectCardのような特殊なハードウェアを使う場合では、そのハードウェアが繋がっている閉じたシステムでしか使用できないし、次々と新しいデータが降り注いでくる放送に対応するハードウェアを作り続けるのは事実上不可能である。これらは、特にPCでの使用を前提とした場合、致命的な欠点となる。

【0010】IRDの場合、IEEE1394によるデータ伝送が前提となるため、FDやCD-ROMで使われていたような物理フォーマットの規格外の使い方や、MacroVisionにあるような映像信号の規格外の信号を使うような、媒体や通信路の物理特性を利用したプロテクトは利用できない。

【0011】IEEE1394は、そのプロトコルの性質上、1対1通信であっても、全てのノードにそのデータが見えてしまう。よって、プロトコルアナライザなどによるデータの横取りが可能である。また、IEEE1394はスターおよびツリー構造の接続が可能であり、またPlug & Play、Hot Plug機能を有しているので、PCをその通信網に後から接続することは簡単に出来てしまう。つまり、IRDなどのAV機器のデジタル出力は、PCがIEEE1394接続のどこかに接続することで見れてしまう。

【0012】この問題に対する対策として、IEEE1394におけるコピープロテクト技術は進展中である。IEEE1394に接続されたどのデバイス同士でも、他の接続したデバイスによる盗み見に対し安全なデータの授受が出来る。これは現在規格策定中であり、どの程度の暗号化が為されるかは未定になっている。ただし、何れにしても、このコピープロテクトは伝送路の暗号化に限定されている。従って、装置の内部ではこれは解読され、平文として装置内部を流れたり蓄積される。完成民生機器の場合はDAT等の例に見られるようにある程度メーカで対応できるが、PC用のデータ放送も考えられており、またPCでのAVコンテンツ再生も可能であることから、PC接続は考慮する必要がある。PC接続においては、以下のような問題が生じる。

【0013】PCはハードウェア、ソフトウェアの交換、増設がユーザレベルで可能なため、DATのようなコピープロテクトでは、暗号化されていないデータがPC内部を流れる際、そのデータを横取りして世代管理領域を書き換えるなどの不正が非常に簡単に行える。また、暗号化をしても、これを解読するためのプログラムは開発可能であるため、安易な暗号化は危険である。特に暗号キーのやり取りをする際にキーを盗み見されると、いくら暗号化しても意味が無い。従来のPCの場合、どのようなアルゴリズムを駆使してやり取りをしても、その暗号キーは少なくともメモリ上のどこかに存在し、ないしはPCの内部バスであるPCIバスなどを必ず通ることになるので、これを盗み見される可能性は否定できない。

【0014】即ち、コンテンツがPCに取り込まれた際、メモリ、PCIバス、ハードディスク、DVD-RAMなどの何れかには必ず平文（暗号化されていない）データが存在し、また暗号化されていない鍵が存在する。このデータを別の媒体にコピーすることはプログラムの的には極めて簡単で、更にこのプログラムをネットワーク上で配布したりウィルスに仕立てるなどして広めることも簡単に可能である。よって、データをPCで取り込むというだけで、不正コピーの可能性が従来に比べて飛躍的に高くなることになる。

【0015】また、デジタル衛星放送のコンテンツをPCで使用する際には、はじめからPCでの使用が前提と

なるが、将来IEEE1394が高度な暗号化をして通信路での安全性を確保しても、PC内部での使用においてPCIバスの部分に解読後のデータが流れることになるので、ウィルスなどの悪意のあるプログラムから守ることが出来ない。

【0016】これに対して、DVD-ROMが使用している手法は、比較的安全であるとされる。DVDドライブと、データを出力するMPEG-2デコーダボードの間はPCIバスおよびIDEバスが介在するが、この間の通信は「認証」と呼ばれるプロセスを経た後、この認証によって作成した暗号キーを使って暗号化した上で送信する。

【0017】認証は、暗号化技術の手法としては一般的なものである。これは、認証をする各々が、盗み見される可能性のある通信路のみを使って通信し、お互いが信頼できる相手であることを確認するための手法である。最も簡単なものとしては、公開暗号鍵の手法を用いるものがある。これは、自分の秘密鍵で自分が発生させた乱数を暗号化して相手に送り、相手側にこれを解読させて相手側に相手側の秘密鍵で暗号化して自分に送らせ、これを解読して最初の乱数と一致するかどうかを見る、というものである。DVDの場合ではもう少し複雑で、認証をしようとする二者が公平な第三者である認証機関より秘密鍵と公開鍵の提供を受け、認証作業において、これが第三者から提供されたものであることを確認するためのアルゴリズムが加わる。これらのアルゴリズムの特徴は、通信路を盗み見してもそのデータは暗号化されており、しかもそれを解くための鍵はソフトウェア的に解析できないところに置かれる（通常はROMに焼かれる）ため、ハードウェアを分解するなどしない限り解読困難である。こうして認証を行った後、その認証情報を元にしてお互いが暗号鍵を内部で生成し、実際のデータはこの暗号鍵を使って暗号化した上でやり取りする。このため、実際のデータを暗号化する暗号鍵は通信路に現れないため、第三者による鍵の入手は不可能になる。

【0018】従来例として最も本発明に近い上記のDVD-ROMにおける手法では、通常のコマンドでは見ることが出来ないメディア固有のID領域、コンテンツ毎の暗号キー領域が設定されており、メディアをどのドライブに入れてもこの情報を単独で読み出すことは出来ない、という特性を利用している。これにより、認証のための情報や暗号キーはドライブによりコントロールされる。しかし、放送や通信を前提とした場合は、認証や暗号化・復号化に必要な情報は全て放送や通信で送る必要がある。このため、DVD-ROMにおける「通常のコマンドでは見ることが出来ない」という条件が崩れ、通信路をスヌープすることにより暗号キーを盗まれる可能性が飛躍的に高まるため、使用することが出来ない。

【0019】また、もし安全にデータを蓄積できた場合でも、それを活用する段階で同じようにデータがメモリ

10

20

30

40

50

にロードされると同様の問題が生じてしまう。ロードの段階でPC Iバスおよびメモリに平文データが現れてしまうため、これを盗まれる可能性が生じる。

【0020】以上のように、IRDからPC等の情報処理機器へデータ伝送をする場合、従来の技術ではコピープロテクト技術は不十分である。

【0021】本発明の目的は、パーソナルコンピュータ等の情報処理機器にて取り扱われるコンテンツデータやプログラム等の不正使用を防止することが可能な情報処理技術を提供することにある。

【0022】本発明の他の目的は、不正使用を懸念することなく、パーソナルコンピュータ等の情報処理機器を用いたコンテンツデータやプログラム等の処理システムの構築を実現することが可能な情報処理技術を提供することにある。

【0023】

【課題を解決するための手段】本発明では、所望の情報伝送路を介して記憶装置と任意の周辺機器の間、および周辺機器間にて情報の授受を行うように構成された情報処理装置において、記憶装置および周辺機器の各々には、情報伝送路を経由して情報の授受を行う相手側を認証する第1の機能、および情報伝送路を経由して授受される情報の暗号化および復号化を行う第2の機能の少なくとも一方を備えた構成とする。

【0024】より具体的には、一例として、PCにてIRD等を備えた有料衛星放送の受信システムを構築する場合、PC内部にあるHDDを、認証と暗号化の機能を搭載したインテリジェントタイプとする。IRD側にも認証機能を持たせ、HDDへは暗号化して送信する。HDDからコンテンツ等のデータを、プログラムやMPEG-2デコーダなどの外部に出す際は、その相手との認証を行い、暗号化してデータを渡す。データを渡された相手は、コピーからの防衛を行いつつデータを処理する。これにより、バス等のデータ転送経路を通るデータを全て暗号化し、かつ暗号鍵そのものも暗号化してやり取り出来るため、安全なデータ伝送が出来る。

【0025】

【発明の実施の形態】以下、本発明の実施の形態を図面を参照しながら詳細に説明する。

【0026】（実施の形態1）図1は、本発明の一実施の形態である情報処理装置の構成の一例を示す概念図である。本実施の形態では、一例として、パーソナルコンピュータ等の情報処理装置を用いて、たとえば有料衛星放送の受信システムを構成する場合を例に採って説明する。

【0027】有料衛星放送等の受信を行うアンテナ8は有料衛星放送のセキュリティ管理等を行うIRD1に接続されており、さらにIRD1はIEEE1394バス2を通してパーソナルコンピュータ（PC）3に接続している。

(4)

特開平11-161165

【0028】PC3の内部では、一例として、PCIバス5を介して、IEEE1394バス2とのI/F制御等を行うIEEE1394コントローラ4、IRD1にて受信されたデータ等の格納を行う記憶装置（HDD）6、全体の制御を行うCPU7、CPU7を制御するプログラムやデータ等が格納される主記憶7a等を接続した構成となっている。

【0029】本実施の形態の場合、IRD1は内部にIEEE1394バス2とのI/F制御等を行うIEEE1394コントローラ11と、IEEE1394バス2に送出されるデータの暗号化や、データの送信相手の認証等の動作を行う認証・暗号化・復号化ユニット12を有している。

【0030】一方、HDD6の内部には、PCIバス5との間のI/F制御を行うバスコントローラ13と、このバスコントローラ13を介して外部との間で授受されるデータの暗号化／復号化、さらにはデータ授受の相手の認証等の動作を行う認証・暗号化・復号化ユニット14を備えている。

【0031】また、PC3において、PCIバス5には、MPEG-2デコーダ9が接続され、このMPEG-2デコーダ9は、PCIバス5を経由して授受されるデータの暗号化／復号化、相手側の認証等の動作を行う認証・暗号化・復号化ユニット15、が設けられ、復号されたデータは、アナログTV出力10を経由してディスプレイ10aに出力される構成となっている。

【0032】HDD6内部の認証・暗号化・復号化ユニット14は、IRD1内部の認証・暗号化・復号化ユニット12との間で、IEEE1394コントローラ11、IEEE1394バス2、IEEE1394コントローラ4、PCIバス5を通じた情報の授受により認証を行い、これによって得たキーで暗号化した上で受信したコンテンツ等のデータをHDD6に送る。この際、IEEE1394バス2、PCIバス5を経由するのでここでデータを盗み見ることは可能であるが、認証を経て暗号化されているので解読できない。

【0033】本実施の形態の場合、IEEE1394規格にのみ頼る暗号化との違いは、PC3の内部においても暗号化が保たれていることである。IEEE1394規格の場合は、IEEE1394コントローラ11とIEEE1394コントローラ4との間の途中の通信経路のみ暗号化され、PC3内部のPCIバス5では平文でデータが流れる。即ち、PCIバス5のスヌープでデータを盗み見る事が出来る。これに対し、本実施の形態では、IRD1からHDD6に送出されるデータは、IRD1の側の認証・暗号化・復号化ユニット12に暗号化された後に送出されるため、HDD6の内部に入るまで暗号化されたままなので、PCIバス5においてもデータを盗み見る事が出来ない。尚、認証の詳細については実施の形態3で説明する。

【0034】認証を経ない一般的な暗号化では、解読キーが暗号化されないまま信頼できないPC Iバス5やIEEE1394バス2を通ることになるので、解読キーを得た第三者がデータをコピーすることが可能になってしまうが、本実施の形態においてはこれらの信頼できないバスを経由しても解読キーは暗号化して送信されるため、第三者は解読キーを入手することが出来ない。このため第三者がデータを解読するにはキーアタックを行うしかないが、解読キーの長さは幾らでも長く出来るため、危険度に応じてキーを長くすれば安全である。ここで、一般的にはキーの解読はキーの長さに応じて指数関数的に難しくなることが知られていることを指摘しておく。

【0035】HDD6に貯えられたデータは、HDD6内部の認証・暗号化・復号化ユニット14を通じてしかやり取りすることが出来ない。したがって、ユーザは、例えば自分のコンピュータといえども、HDD6の許可無しにデータを見ることは出来ない点に本実施の形態の大きな特徴がある。

【0036】（実施の形態2）同じく図1で、PC3のHDD6へ蓄積したデータが映像データであった場合のデータ出力処理の一例を説明する。

【0037】HDD6に蓄積されたデータはPC Iバス5を通じてMPEG-2デコーダ9に送られ、アナログTV出力10を経由してディスプレイ10aに出力される。HDD6とMPEG-2デコーダ9の間のデータやり取りには、HDD6側の認証・暗号化・復号化ユニット14とMPEG-2デコーダ9側の認証・暗号化・復号化ユニット15との間での認証が必要であり、データは暗号化される。この際、PC Iバス5を経由するが、暗号化されているのでデータは利用できない。また、認証されているので間違った相手にデータを送ることはない。

【0038】HDD6からデータを取り出すにはHDD6との認証に成功する必要がある、そのためには認証機関より与えられた公開暗号鍵が必要である。即ち、公開暗号鍵をコントロールすることにより、データを使ってよいデバイスが制限される。実際には、公開暗号鍵はMPEG-2デコーダ9が持っているが、MPEG-2デコーダ9を製造するメカが認証機関から鍵を契約により取得する。取得のためには、解読後のデータをボード内部でのみ使うようにハードウェア的な制限を加えるなど、認証機関が与える一定の条件をクリアしなければならないようにする。これにより、コンテンツメカは、PC3に送ったデータの使われ方、コピーに関するコントロールを実現できる。

【0039】これは、PC3におけるDVD-Videoの再生の一般的構成と極めて似ているが、データの保存元であるHDD6は書き換え可能であり、更に記憶媒体が着脱不可能である点が大きく異なる。書き換え可能

である点に関しては、HDD6が貯えるデータはどこからコピーしてきたものであるため、少なくともそのデータは純粋に論理的なデータである。つまり、CD-ROMやFDDにおける物理的なコピープロテクトは原理的に不可能であり、DVD-ROMにおけるディスクIDのような特定のデバイス固有の仕掛けも同様に不可能である。また、記憶媒体が着脱不可能である点に関しては、着脱可能な媒体の場合、媒体のどこに暗号鍵を置いても、外して別の装置に掛けることでその暗号鍵が読めてしまうのに対し、媒体が着脱不可能なのであくまでもHDD6内部の認証を通してしか情報を入手することが出来ず、暗号鍵は安全である。

【0040】MPEG-2映像に限らず、データを扱う機器一般にこれは適用できる。例えば相手がAC-3デコーダアンプである場合など、音声データであった場合、認証を経していないアンプでは再生できない。また、相手がディスプレイであった場合、表示は出来てもアナログ出力が出ないようにする、アナログコピーガードを掛ける、等のコントロールをディスプレイ側ですることが出来るし、認証を得ていないディスプレイでは再生できない。

【0041】また、複数のHDDの間でコピーをする場合、認証機能の無いHDDにコピーすることは出来ないようにするか、暗号化されたままコピーされるように設定できる。後者では、この復号キーは認証機能のあるHDDのみが所有しているため、最終的にデータを使用するところ、実施の形態2ではMPEG-2デコーダ9においてデータを解読することが出来ず、結果としてコンテンツメカはコピーコントロールが出来たことになる。

【0042】以上のように、最終的にユーザがデータを使うためのハードウェアを認証機関が指定すること、即ち認証鍵を配布するかしないかをコントロールすることにより、データをユーザが使うための条件をコントロールすることが出来る。

【0043】（実施の形態3）図2は、本発明の情報処理装置にて使用される認証アルゴリズムの一例を示すフローチャートである。

【0044】認証は、実施の形態1においてはIRD1とHDD6との間で、実施の形態2においてはHDD6とMPEG-2デコーダ9との間で行われる。

【0045】これは、原則的には一般的に行われている認証のアルゴリズムと同一のものを使える。図2では、最も簡単な例を示している。IRD1とHDD6が認証を行う例を示す。

【0046】IRD1側には秘密鍵K_{pr} (IRD) および公開鍵K_{pu} (IRD)、HDD6側には秘密鍵K_{pr} (HDD) および公開鍵K_{pu} (HDD) を持つ。また、双方が共通の暗号化アルゴリズムC (Key, Dest) および復号化アルゴリズムC' (Key, De

st)を持つ。ここでKeyは暗号化鍵、Destはターゲットデータである(ステップS1)。

【0047】アルゴリズムCと公開鍵Kpu、秘密鍵Kprの間には、以下のような関係がある。即ち、アルゴリズムCで秘密鍵Kprをキーとして暗号化したデータC(Kpr, Dest)に対して公開鍵Kpuを用いて復号化した結果であるC'(kpu, C(Kpr, Dest))は一致する。またこの逆に、アルゴリズムCで公開鍵Kpuをキーとして暗号化したデータC(Kpu, Dest)に対して秘密鍵Kprをキーとして復号化した結果であるC'(Kpr, C(Kpu, Dest))は一致する。即ち、秘密鍵で暗号化したデータは公開鍵で解け、公開鍵で暗号化したデータは秘密鍵で解ける。また、アルゴリズム、公開鍵、暗号化されたデータの三つを第三者に知られても、これから平文データないしは暗号鍵を求めることは、数学的に極めて困難である。

【0048】HDD6がIRD1にデータの転送要求を出す時、HDD6はIRD1に対し、自分の公開鍵Kpu(HDD)を送信する(ステップS2)。

【0049】IRD1はこれを受け取ると、自身で乱数R(IRD)を発生させ、これを種としてKpu(HDD)を暗号化する。これをC1=C(Kpu(HDD), R(IRD))と表す(ステップS3)。IRD1はこの結果を、自分の公開鍵であるKpu(IRD)と共に送信する(ステップS4)。

【0050】HDD6は受け取った暗号であるC1を自分の暗号鍵で復号化する。これをR'(IRD)=C'(Kpr(HDD), C1)で表す。これは、元のR(IRD)に一致するはずである。HDD6はこれを相手の公開鍵Kpu(IRD)で暗号化した結果であるC2=C(Kpu(IRD), R(IRD))をIRD1に送信する。同時に、自身で乱数R(HDD)を発生させ、これを相手の公開鍵で暗号化した結果であるC3=C(Kpu(IRD), R(HDD))を送信する(ステップS5、ステップS6)。

【0051】IRD1はC2を復号化した結果であるR''(IRD)=C'(Kpr(IRD), C2)と最初に自身が発生させた乱数であるR(IRD)が一致するかどうかを調べる。一致すれば、IRD1にとってHDD6は認証されたことになる。これが成功すると、IRD1はC3を復号化する。これをR'(HDD)=C'(Kpr(IRD), C3)で表す。R'(HDD)はR(HDD)に一致するはずである。IRD1はこれを暗号化してHDD6に送信する。これをC4=C(Kpu(HDD), R'(HDD))で表す。同時に、IRD1はデータ送信用のキーであるKを生成し、C5=C(Kpu(HDD), K)として送信する(ステップS7、ステップS8)。

【0052】HDD6はC4を解読し、R''(HDD)

(6)

特開平11-161165

10

=C'(Kpr(HDD), C4)を生成する。これがR(HDD)と一致すれば、HDD6にとってIRD1は認証されたことになる。これを受けて、HDD6はK=C'(Kpr(HDD), C5)を生成する。

【0053】以上の操作により、お互いはお互いを認証し、実際のデータ暗号化のための共通キーKを共有することが出来たことになる。以後のデータ送信は共通鍵暗号アルゴリズムと共通キーKを使ってやりとりする。

【0054】たとえば、IRD1にて受信した有料衛星放送のコンテンツデータ(Data)をIRD1からHDD6へ送出する場合には、たとえば、図3に例示されるように、データストリームを、たとえば所定のビット長毎に共通キーKを用いて、認証・暗号化・復号化ユニット12にて、C6=C(Data, K)として暗号化されたデータストリームを生成した後、このC6をHDD6へと送り出す(ステップS10、ステップS11)。

【0055】このC6を受信したHDD6側では、C'(C6, K)にて、C6を復号化して元のコンテンツデータ(Data)を得て記憶媒体に格納する(S12)。

【0056】また、HDD6に格納されたコンテンツデータを、MPEG-2デコーダ9に送信する場合には、送信側のHDD6は、図2におけるIRD1と等価な動作を行い、受信側のMPEG-2デコーダ9は、図2におけるHDD6と等価な動作を行うことで、HDD6とMPEG-2デコーダ9は互いに他を認証できるとともに、PCIバス5を流れるコンテンツデータは両者の固有の共通キーKにて暗号化された状態となるため、PCIバス5を流れるコンテンツデータの不正使用を確実に防止できる。

【0057】同様に、IRD1から、PCIバス5を経由して、直接的に、MPEG-2デコーダ9にコンテンツデータ(Data)を送出してディスプレイ10aへの再生出力を行わせる場合には、受信側のMPEG-2デコーダ9が、図におけるHDD6と等価な動作を行うことで、IRD1とMPEG-2デコーダ9は互いに他を認証できるとともに、PCIバス5を流れるコンテンツデータは両者の固有の共通キーKにて暗号化された状態となるため、PCIバス5を流れるコンテンツデータの不正使用を確実に防止できる。

【0058】以上のように、本実施の形態の通信では、通信路(IEEE1394バス2やPCIバス5)には双方の公開鍵と暗号化データしかやり取りされない。また、共通鍵は暗号化されてやり取りされる他、公開鍵から秘密鍵を求めることは出来ない。これらより、データを盗んでも鍵が分からないため復号は出来ない。従って、データの不正コピー等の不正使用を確実に防止できる。

【0059】図2の例では、アルゴリズムの最後で、実

50

際のデータの暗号化には共通キーKを用いる暗号アルゴリズムを用いている。これは、通常、公開暗号鍵アルゴリズムは極めて速度が遅く、映像データ等のコンテンツなどの多量のデータをやり取りするには適していないためである。すなわち、本実施の形態では、認証は公開暗号鍵で行い、データの暗号化は共通キーKで行い、共通キーKのやり取りは認証に基づいた公開暗号鍵で行うことも本発明に含まれる。

【0060】以上本発明者によってなされた発明を実施の形態に基づき具体的に説明したが、本発明は前記実施の形態に限定されるものではなく、その要旨を逸脱しない範囲で種々変更可能であることはいうまでもない。

【0061】たとえば、上述の例では、不正使用からの保護対象として、コンテンツ等のデータに適用した場合について説明したが、これに限らず、たとえば、IRDを経由で配付されるゲームやビジネス等のソフトウェア等の保護にも適用することができる。その場合には、当該ソフトウェアの受信部分（たとえばIRD）から実行部分（CPUや主記憶、あるいはソフトウェア実行専用に接続された周辺機器）までの間におけるデータ転送経路における暗号化を行うようにすればよい。

【0062】

【発明の効果】本発明の情報処理装置によれば、パーソナルコンピュータ等の情報処理機器にて取り扱われるコ*

*ンテンツデータやプログラム等の不正使用を防止することができる、という効果が得られる。

【0063】本発明の情報処理装置によれば、不正使用を懸念することなく、パーソナルコンピュータ等の情報処理機器を用いたコンテンツデータやプログラム等の処理システムの構築を実現することができる、という効果が得られる。

【図面の簡単な説明】

【図1】本発明の一実施の形態である情報処理装置の構成の一例を示す概念図である。

【図2】本発明の情報処理装置にて使用される認証アルゴリズムの一例を示すフローチャートである。

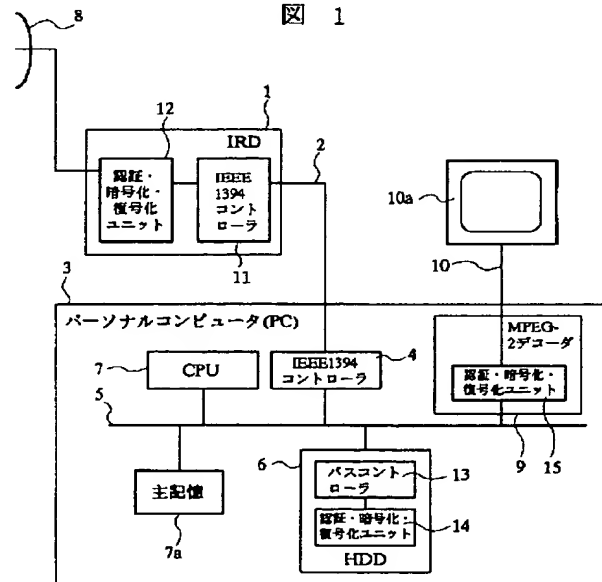
【図3】本発明の情報処理装置におけるデータの暗号化の過程の一例を示す概念図である。

【符号の説明】

1…IRD（周辺機器）、2…IEEE1394バス、3…パーソナルコンピュータ、4…IEEE1394コントローラ、5…PCIバス（情報伝送路）、6…記憶装置、7…CPU、7a…主記憶、8…アンテナ、9…MPEG-2デコーダ（周辺機器）、10…アナログTV出力、10a…ディスプレイ、11…IEEE1394コントローラ、12…認証・暗号化・復号化ユニット（第1の機能、第2の機能）、13…バスコントローラ、14…認証・暗号化・復号化ユニット（第1の機能、第2の機能）、15…認証・暗号化・復号化ユニット（第1の機能、第2の機能）。

【図1】

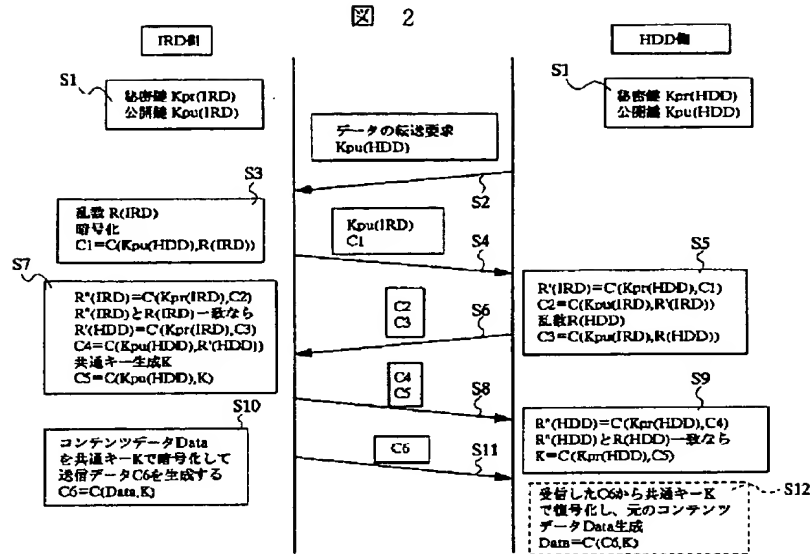
図 1



2: IEEE1394バス
5: PCIバス
8: アンテナ

10: アナログTV出力
10a: ディスプレイ

【図2】



【図3】

図 3

